

Getting something out of nothing

Hoi-Kwong Lo *

*Center for Quantum Information and Quantum Control
Dept. of Electrical & Computer Engineering & Dept. of Physics
University of Toronto, 10 King's College Road
Toronto, Ontario, CANADA, M5S 3G4.*

Abstract

We study quantum key distribution with standard weak coherent states and show, rather counter-intuitively, that the detection events originated from vacua can contribute to secure key generation rate, over and above the best prior art result. Our proof is based on a communication complexity/quantum memory argument.

1 Introduction

The best-known application of quantum cryptography is quantum key distribution (QKD) [1]. The goal of QKD is to allow two parties, Alice and Bob, to share a common string of secret in the presence of an eavesdropper, Eve. Such a key can subsequently be used for, for example, perfectly secure communications via the so-called one-time-pad. Unlike conventional cryptography, the security of QKD is guaranteed by the fundamental law of physics—the Heisenberg uncertainty principle. The best-known protocol for QKD is the Bennett-Brassard protocol (BB84) [1]. In BB84, Alice sends Bob a sequence of single photons in one of the four polarizations (vertical, horizontal, 45-degree and 135-degree) and Bob randomly performs a measurement in one of the two conjugate bases. In principle, the security of QKD has been proven in a number of papers including [2, 3, 4].

For practical implementations, an attenuated laser pulse (a so-called weak coherent state) is often used as the source. The security of QKD with a rather generic class of imperfect devices has been proven in GLLP [5], following the earlier work [6]. Recently, Hwang [7] has proposed a decoy state idea for improving the performance (i.e., the key generation rate and distance) of QKD systems. We [8] have demonstrated rigorously how the decoy state idea can be combined with GLLP to obtain a key generation rate (per pulse emitted by Alice) which is lower bounded by:

$$S \geq Q_{\text{signal}} \{-H_2(E_{\text{signal}}) + \Omega_1[1 - H_2(e_1)]\}, \quad (1)$$

where Q_{signal} and E_{signal} are respectively the gain and quantum bit error rate (QBER) of the signal state, Ω_1 and e_1 are respectively the fraction and QBER of detection events by Bob that have originated from single-photon signals emitted by Alice. Here, the gain means the ratio of Bob's detection events to Alice's total number of emitted signals.

*Email: hklo@comm.utoronto.ca

[Decoy state QKD has subsequently been investigated by Wang [9] and by Harrington [10].]

The key goal of this paper is to increase the above key generation rate in Eq. 1 by a term $Q_{signal}\Omega_0$ where Ω_0 is the fraction of detection events of Bob that have originated from vacua emitted by Alice. More concretely, we have the following main Theorem.

Theorem 1 The key generation of an efficient BB84 scheme is given by:

$$S \geq Q_{signal}\{-H_2(E_{signal}) + \Omega_0 + \Omega_1[1 - H_2(e_1)]\}, \quad (2)$$

where Ω_0 is the fraction of detection events by Bob that has originated from the vacuum signals emitted by Alice. In other words, we find that each detection event by Bob that has originated from a vacuum (i.e., nothing) emitted by Alice automatically contributes to a bit of secure key over and above the prior art result (Eq. 1) presented in [5] and also [8].

Before we embark on a detailed discussion, let us check for the consistency of our result. Naively, one might think that our suggestion that the vacuum will contribute to a secure key is an insane idea because if nothing is emitted by Alice, what is the origin of security? We remark that the vacuum *alone* does *not* contribute to a secure key. More concretely, suppose all the signals sent by Alice are vacua and there are no background events. Then, $\Omega_0 = 1$, $\Omega_1 = 0$, and $E_{signal} = 1/2$. Therefore, from Eq. 2, we get the lower bound 0 for the key generation rate. The reason is that the term Ω_0 is exactly cancelled by the error correction term $-H_2(E_{signal})$.

What Eq. 2 does say is that no privacy amplification is needed for the vacua state. This is intuitively clear because Eve cannot have any a priori information on Alice's bit, if nothing is emitted from Alice's laboratory.

Now, let us prove our main result (Eq. 2). We shall use the method of communication complexity. As noted by Ben-Or [3] and by Renner and Koenig [11], the number of rounds of universal hashing needed for privacy amplification in QKD is at most given by any upper bound to the size of Eve's quantum memory which contains information on the key. In other words, we have, informally:

Theorem 2 [3, 11]: The key generation rate in QKD

$$S \geq N - \mathcal{S}_{Eve} \quad (3)$$

where N is the size of the sifted key shared between Alice and Bob and \mathcal{S}_{Eve} is the size of Eve's quantum memory. [A more formal definition involving the relevant ϵ and δ can be found as Eq. (11) in [11].]

Remark: Note that Theorem 2 only gives a lower bound to the key generation rate because it does not consider the possibility of advantage distillation in QKD [12].

In summary, all we need to compute (a lower bound to) the key generation rate is to work out the size of Eve's quantum memory.

Proof of Theorem 1: Now, note that Eve has two pieces of information on the key. The first piece, which is strictly quantum, comes from Eve's eavesdropping attack during the quantum transmission from Alice to Bob. The second piece is classical and comes from the classical error correction part.

We argue that the first piece, from eavesdropping the quantum transmission, consists of two parts: single-photon part and multi-photon part. It should be emphasized that the vacua signals do *not* contribute at all. This is because, since Alice is emitting nothing, Eve cannot possibly learn anything about Alice's key. Eve can influence and, in fact, decide on Bob's key by sending her own photons into Bob's detector. However, Bob's key does not really tell Eve anything about Alice's key.

Let us consider the multi-photon part first. We take the most conservative assumption that Eve has all the information on all multi-photon signals. Her quantum memory

size on the multi-photon part is then given by $Q_{\text{signal}}\Omega_m$. Here, Ω_m is the fraction of detection events of Bob that have originated from multi-photon signals. Note that $\Omega_0 + \Omega_1 + \Omega_m = 1$. The single-photon part is given by simply $Q_{\text{signal}}\Omega_1 H_2(e_1^{\text{phase}})$, where e_1^{phase} is the phase error rate of the single-photon signals. From Shor-Preiskill's proof [4], $e_1^{\text{phase}} = e_1$, which is the bit-flip error rate for the single-photon signals. So, the quantum memory for single-photon part is actually given by $Q_{\text{signal}}\Omega_1 H_2(e_1)$. Adding the two parts, the first piece of Eve's information has a memory size $Q_{\text{signal}}[\Omega_1 H_2(e_1) + \Omega_m]$. The second piece of Eve's information, which comes from classical error correction, is asymptotically given by $Q_{\text{signal}}H_2(E_{\text{signal}})$.

In summary, adding the two pieces together, the total quantum memory size of Eve is given by $\mathcal{S}_{\text{Eve}} = Q_{\text{signal}}[H_2(E_{\text{signal}}) + \Omega_1 H_2(e_1) + \Omega_m]$.

Now, the length of the sifted key (per pulse emitted by Alice) shared by Alice and Bob is $N = Q_{\text{signal}}[\Omega_0 + \Omega_1 + \Omega_m]$. Therefore, the number of secure key bits (per pulse emitted by Alice) is given by

$$\begin{aligned} S &\geq N - \mathcal{S}_{\text{Eve}} \\ &= Q_{\text{signal}}\{-H_2(E_{\text{signal}}) + \Omega_0 + \Omega_1[1 - H_2(e_1)]\}. \end{aligned} \quad (4)$$

which is precisely Eq. (2). This concludes the proof of our Theorem 1.

In summary, we have increased the key generation from Eq. (1) in the prior art result [5] to Eq. (2) by showing that, rather counter-intuitively, the detection events due to vacua contribute directly to the secure key. What is interesting about this result is that it is based on a communication complexity approach and is not entirely clear whether it can be derived from an entanglement distillation approach. In future, it will perhaps be interesting to rephrase this result in the general framework of Γ states [13], which generalizes the entanglement distillation approach.

Acknowledgements

We thank helpful discussions with colleagues including J. Batuwantudawe, Jean-Christian Boileau, Debbie Leung, John Preskill and Kiyoshi Tamaki. This part is financially supported in part by funding agencies including CFI, CIPI, CRC program, NSERC, OIT, and PREA. Parts of this paper were written during visits to the Institute of Quantum Information (IQI) at Caltech and to the Isaac Newton Institute, Cambridge, UK, whose kind hospitality is acknowledged.

References

- [1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, IEEE, 1984, pp. 175-179.
- [2] D. Mayers, Journal of ACM, vol. 48, 351 (2001). Available on-line at <http://arxiv.org/abs/quant-ph/9802025>. A preliminary version in D. Mayers, Quantum key distribution and string oblivious transfer in noisy channel, *Advances in Cryptology — Proceedings of Crypto' 96*, Lecture Notes in Computer Science, vol. 1109, Springer-Verlag, 1996, pp. 343-357; H.-K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, *Science*, vol. 283, (1999), pp. 2050-2056; also available at <http://xxx.lanl.gov/abs/quant-ph/9803006>; E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, A proof of security of quantum key distribution, *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*, ACM Press, New York, 2000, p. 715

- [3] M. Ben-Or, Simple security proof for quantum key distribution. Online presentation available at <http://www.msri.org/publications/ln/msri/2002/qip/ben-or/1/index.html>
- [4] P. W. Shor and J. Preskill, Simple proof of security of the BB84 quantum key distribution scheme, Phys. Rev. Lett. vol. 85, (2000), pp. 441-444.
- [5] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Security of quantum key distribution with imperfect devices, Quantum Information and Computation. Vol. 4, No.5 (2004) 325-360; available at <http://xxx.lanl.gov/abs/quant-ph/0212066>
- [6] Inamori, H., Lütkenhaus, N. & Mayers, D. Los Alamos e-Print archive (available at <http://arxiv.org/abs/quant-ph/0107017>).
- [7] W.-Y. Hwang, “*Quantum Key Distribution with High Loss: Toward Global Secure Communication*”, Phys. Rev. Lett. 91, 057901 (2003).
- [8] H.-K. Lo, X. Ma and K. Chen “*Decoy State Quantum Key Distribution*”, <http://lanl.arxiv.org/abs/quant-ph/0411004>. Preliminary results were presented in Proceedings of IEEE ISIT 2004, July 2004 and various scientific conferences such as Fields Institute Conference on Quantum Information and Quantum Control, <http://www.fields.utoronto.ca/programs/scientific/04-05/quantumIC/abstracts/lo.ppt>
- [9] Xiang-Bin Wang, “*Beating the PNS attack in practical quantum cryptography*”, <http://arXiv:quant-ph/0411047>, v4 28 Jan 2005.
- [10] J. Harrington, poster presentation at QIP 2005, Jan 2005.
- [11] R. Renner and R. Koenig, “Universally composable privacy amplification against quantum adversaries,” On-line available at <http://xxx.lanl.gov/abs/quant-ph/0403133>
- [12] D. Gottesman and H.-K. Lo, Security of quantum key distribution with two-way classical communications, IEEE Transactions on Information Theory, Vol. 49, No. 2, p. 457 (2003). <http://xxx.lanl.gov/abs/quant-ph/0105121>
- [13] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, “secure key from bound entanglement”, On-line available at <http://xxx.lanl.gov/abs/quant-ph/0309110>